



# FortiAnalyzer - Release Notes

Version 6.0.0

**FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTIGATE COOKBOOK**

<http://cookbook.fortinet.com>

**FORTINET TRAINING SERVICES**

<http://www.fortinet.com/training>

**FORTIGUARD CENTER**

<http://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<http://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



July 13, 2018

FortiAnalyzer 6.0.0 Release Notes

05-600-474412-20180713

# TABLE OF CONTENTS

<b>Change Log</b>	<b>5</b>
<b>Introduction</b>	<b>6</b>
Supported models	6
Minimum screen resolution	6
What's new in FortiAnalyzer version 6.0.0	7
Incident Detection & Response	7
FortiAnalyzer High Availability	7
Secure Syslog Forwarding	7
<b>Special Notices</b>	<b>8</b>
FortiManager features disabled when FortiAnalyzer HA enabled	8
Updated Widgets for Fortinet Security Fabric	8
Hyper-V FortiAnalyzer-VM running on an AMD CPU	8
SSLv3 on FortiAnalyzer-VM64-AWS	8
Pre-processing logic of ebtime	8
<b>Upgrade Information</b>	<b>10</b>
Upgrading to FortiAnalyzer 6.0.0	10
Downgrading to previous versions	10
Firmware image checksums	10
FortiAnalyzer VM firmware	10
SNMP MIB files	12
<b>Product Integration and Support</b>	<b>13</b>
FortiAnalyzer version 6.0.0 support	13
Feature support	15
FortiGate Management	16
Language support	16
Supported models	17
<b>Resolved Issues</b>	<b>25</b>
Device Manager	25
FortiView	25
Log View	25
Reports	26
System Settings	26
NOC	27
Others	27
System Settings	27
Common Vulnerabilities and Exposures	27
<b>Known Issues</b>	<b>28</b>
Device Manager	28

---

Event Management .....	28
FortiView .....	29
Log View .....	29
NOC .....	30
Reports .....	30
System settings .....	30
Others .....	31

# Change Log

Date	Change Description
2018-04-18	Initial release of 6.0.0.
2018-05-01	Added 5.6.4 support to <i>Product Integration &amp; Support &gt; FortiOS</i> .
2018-06-27	Added note to <i>Product Integration &gt; Supported Models &gt; FortiGate Models &gt; 6.0 &gt; FortiGate Hardware Low Encryption</i> .
2018-07-13	<p>Added <i>FortiManager features disabled when FortiAnalyzer HA enabled</i> to <i>Special Notices</i>.</p> <p>Updated <i>Product Integration and Support &gt; FortiGate Management</i> to clarify that FortiAnalyzer HA is not supported when FortiManager features are enabled.</p> <p>Updated <i>Product Integration and Support &gt; Language Support</i> to clarify that you can create your own language translation files for Russian, Hebrew, and Hungarian, and import the language translation files into FortiAnalyzer by using the CLI.</p>

# Introduction

This document provides the following information for FortiAnalyzer version 6.0.0 build 0092:

- [Supported models](#)
- [What's new in FortiAnalyzer version 6.0.0](#)
- [Special Notices](#)
- [Upgrade Information](#)
- [Product Integration and Support](#)
- [Resolved Issues](#)
- [Known Issues](#)

For more information on upgrading your FortiAnalyzer device, see the *FortiAnalyzer Upgrade Guide*.

## Supported models

FortiAnalyzer version 6.0.0 supports the following models:

<b>FortiAnalyzer</b>	FAZ-200D, FAZ-200F, FAZ-300D, FAZ-300F, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3700F and FAZ-3900E.
<b>FortiAnalyzer VM</b>	FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-AWS-OnDemand, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).

## Minimum screen resolution

The recommended minimum screen resolution is 1280 x 800. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

## What's new in FortiAnalyzer version 6.0.0

The following is a list of new features and enhancements in FortiAnalyzer version 6.0.0.

### Incident Detection & Response

#### Event Manager 2.0

- From *Event Manager > All Events*, you can now search and filter events, customize columns and save filtered events to a Custom View.
- The secondary *Group By* option from the event handler edit screen provides flexibility on event information organization.
- Built-in event handler to provide threat feed to the FortiOS automation framework.  
You can raise an incident from detected events. The raised incident is listed under the *Incidents* menu for further analysis and evidence collection.

#### SOC Dashboards

- **Fortinet Security Best Practice Dashboard:** a simple CISO dashboard to show a snapshot of the security of your network, including the current security ranking score, industry peer comparison, and security maturity level.
- **New Vulnerability Dashboard:** displays a summary of detected endpoint vulnerabilities along with the detailed FortiGuard information for each critical vulnerability.

#### IOC Enhancements

- IOC scan now includes Traffic logs and DNS logs to provide better detection coverage.
- The IOC Notification Service provides event notification to FortiOS when a compromised host is detected.

### FortiAnalyzer High Availability

Support automatic failover over IP for log redundancy and high system availability.

### Secure Syslog Forwarding

Support forwarding logs in syslog format over TLS/SSL.

# Special Notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer version 6.0.0.

## FortiManager features disabled when FortiAnalyzer HA enabled

If you have FortiManager features enabled on FortiAnalyzer units, and then enable HA for the FortiAnalyzer units, FortiManager features are automatically disabled. FortiManager features are not supported when FortiAnalyzer HA is enabled.

## Updated Widgets for Fortinet Security Fabric

After upgrading FortiAnalyzer from 5.6 to 6.0, the NOC Security Fabric widgets, *Security Fabric Score Summary* and *Historical Security Fabric Scores*, no longer show any data. These two widgets have been replaced by the following widgets: *Security Fabric Rating Report* and *Security Fabric Scores* in FortiAnalyzer 6.0. The two new widgets only support FortiOS 6.0 devices.

## Hyper-V FortiAnalyzer-VM running on an AMD CPU

A Hyper-V FAZ-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel-based PC.

## SSLv3 on FortiAnalyzer-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiAnalyzer-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global
    set ssl-protocol tlsv1
end
```

## Pre-processing logic of ebtime

Logs with the following conditions met are considered usable for the calculation of estimated browsing time:



Traffic logs with `logid` of 13 or 2, when `logid == 13`, `hostname` must not be empty. The `service` field should be either `HTTP, 80/TCP` or `443/TCP`.

If all above conditions are met, then `devid`, `vdom`, and `user` (`srcip` if `user` is empty) are combined as a key to identify a user. For time estimation, the current value of `duration` is calculated against history session start and end time, only un-overlapped part are used as the `ebtime` of the current log.

# Upgrade Information

## Upgrading to FortiAnalyzer 6.0.0

You can upgrade FortiAnalyzer 5.6.0 or later directly to 6.0.0. After upgrade, FortiAnalyzer will rebuild the system database automatically.

If you are upgrading from versions earlier than 5.6.0, you must upgrade to FortiAnalyzer 5.6, then to 6.0.0. We recommend that you upgrade to 5.6.3, the latest version of FortiAnalyzer 5.6



For details about upgrading your FortiAnalyzer, see *FortiAnalyzer Upgrade Guide*.

---

## Downgrading to previous versions

FortiAnalyzer does not provide a full downgrade path. You can downgrade to a previous firmware release via the GUI or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrading process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset all-settings
execute format {disk | disk-ext4}
```

## Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, <https://support.fortinet.com>. To verify the integrity of the download, select the *Checksum* link next to the *HTTPS* download link. A dialog box will be displayed with the image file name and checksum code. Compare this checksum with the checksum of the firmware image.

## FortiAnalyzer VM firmware

Fortinet provides FortiAnalyzer VM firmware images for Amazon AWS, Citrix and Open Source XenServer, Linux KVM, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

### Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available on the AWS marketplace.

## Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains the QCOW2 file for the Open Source Xen Server.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains the Citrix XenServer Disk (VHD), and OVF files.

## Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiAnalyzer VM installation. This package contains QCOW2 that can be used by qemu.

## Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `FAZ_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.hyperv.zip`: Download the package for a new FortiAnalyzer VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Azure.

## Microsoft Hyper-V Server

The files for Microsoft Hyper-V Server have HV in the filenames, for example, `FAZ_VM64_HV-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiAnalyzer VM installation.
- `.hyperv.zip`: Download the package for a new FortiAnalyzer VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.



Microsoft Hyper-V 2016 is supported.

---

## VMware ESX/ESXi

- `.out`: Download either the 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.



For more information see the FortiManager product data sheet available on the Fortinet web site, <http://www.fortinet.com/products/fortimanager/virtual-security-management.html>. VM installation guides are available in the [Fortinet Document Library](#).

---

## SNMP MIB files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiAnalyzer v5.00 file folder.

# Product Integration and Support

## FortiAnalyzer version 6.0.0 support

The following table lists FortiAnalyzer version 6.0.0 product integration and support information:

<b>Web Browsers</b>	<ul style="list-style-type: none"><li>• Microsoft Internet Explorer version 11 or Edge 40 Due to limitation on Microsoft Internet Explorer or Edge, it may not completely render a page with a large set of policies or objects.</li><li>• Mozilla Firefox version 59</li><li>• Google Chrome version 65</li></ul> <p>Other web browsers may function correctly, but are not supported by Fortinet.</p>
<b>FortiOS/FortiOS Carrier</b>	<ul style="list-style-type: none"><li>• 6.0.0</li><li>• 5.6.0 to 5.6.4</li><li>• 5.4.0 to 5.4.8</li><li>• 5.2.0 to 5.2.13</li></ul>
<b>FortiAnalyzer</b>	<ul style="list-style-type: none"><li>• 6.0.0</li><li>• 5.6.0 to 5.6.3</li><li>• 5.4.0 to 5.4.3</li><li>• 5.2.0 to 5.2.9</li><li>• 5.0.0 to 5.0.13</li></ul>
<b>FortiCache</b>	<ul style="list-style-type: none"><li>• 4.2.7</li><li>• 4.2.6</li><li>• 4.1.3</li><li>• 4.0.4</li></ul>
<b>FortiClient</b>	<ul style="list-style-type: none"><li>• 5.6.0 and later</li><li>• 5.4.0 and later</li><li>• 5.2.0 and later</li><li>• 5.0.4 and later</li></ul>
<b>FortiMail</b>	<ul style="list-style-type: none"><li>• 5.4.5</li><li>• 5.4.2</li><li>• 5.3.8</li><li>• 5.2.9</li><li>• 5.1.6</li><li>• 5.0.10</li></ul>

<b>FortiManager</b>	<ul style="list-style-type: none"><li>• 6.0.0</li><li>• 5.6.0 to 5.6.3</li><li>• 5.4.0 to 5.4.3</li><li>• 5.2.0 and later</li><li>• 5.0.0 and later</li></ul>
<b>FortiSandbox</b>	<ul style="list-style-type: none"><li>• 2.5.2</li><li>• 2.5.1</li><li>• 2.5.0</li><li>• 2.4.1</li><li>• 2.4.0</li><li>• 2.3.3</li><li>• 2.3.2</li><li>• 2.2.2</li><li>• 2.1.3</li><li>• 2.0.3</li><li>• 1.4.0 and later</li><li>• 1.3.0</li><li>• 1.2.0 and 1.2.3</li></ul>
<b>FortiSwitch ATCA</b>	<ul style="list-style-type: none"><li>• 5.0.0 and later</li><li>• 4.3.0 and later</li><li>• 4.2.0 and later</li></ul>
<b>FortiWeb</b>	<ul style="list-style-type: none"><li>• 5.9.0</li><li>• 5.8.6</li><li>• 5.8.1</li><li>• 5.8.0</li><li>• 5.7.0</li><li>• 5.6.0</li><li>• 5.5.4</li><li>• 5.4.1</li><li>• 5.3.8</li><li>• 5.2.4</li><li>• 5.1.4</li><li>• 5.0.6</li></ul>
<b>FortiDDoS</b>	<ul style="list-style-type: none"><li>• 4.5.0</li><li>• 4.4.1</li><li>• 4.2.3</li><li>• 4.1.12</li></ul>

<b>FortiAuthenticator</b>	<ul style="list-style-type: none"> <li>• 5.2.2</li> <li>• 5.1.0</li> <li>• 5.0.0</li> <li>• 4.3.0</li> <li>• 4.2.0</li> <li>• 4.1.0</li> <li>• 4.0.0</li> </ul>
<b>Virtualization</b>	<ul style="list-style-type: none"> <li>• Amazon Web Service AMI, Amazon EC2, Amazon EBS</li> <li>• Citrix XenServer 6.2</li> <li>• Linux KVM Redhat 6.5</li> <li>• Microsoft Azure</li> <li>• Microsoft Hyper-V Server 2008 R2, 2012 &amp; 2012 R2</li> <li>• OpenSource XenServer 4.2.5</li> <li>• VMware: <ul style="list-style-type: none"> <li>• ESX versions 4.0 and 4.1</li> <li>• ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0 and 6.5</li> </ul> </li> </ul>



Always review the Release Notes of the supported platform firmware version before upgrading your device.

## Feature support

The following table lists FortiAnalyzer feature support for log devices.

Platform	Log View	FortiView	Event Management	Reports
FortiGate	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓
FortiAnalyzer	✓		✓	
FortiCache	✓		✓	✓
FortiClient registered to FortiGate	✓	✓		✓
FortiClient registered to FortiClient EMS	✓	✓		✓
FortiDDoS	✓	✓	✓	✓
FortiMail	✓		✓	✓
FortiManager	✓		✓	

Platform	Log View	FortiView	Event Management	Reports
FortiSandbox	✓		✓	✓
FortiWeb	✓		✓	✓
Syslog	✓		✓	

## FortiGate Management

You can enable FortiManager features on some FortiAnalyzer models. FortiAnalyzer models with FortiManager features enabled can manage a small number of FortiGate devices, and all but a few FortiManager features are enabled on FortiAnalyzer.



FortiAnalyzer HA is not supported when FortiManager features are enabled.

The following table lists the supported modules for FortiAnalyzer with FortiManager Features enabled:

FortiManager Management Modules	FortiAnalyzer with FortiManager Features Enabled
Device Manager, except firmware and license management	✓
Policy & Objects	✓
AP Manager	✓
FortiClient Manager	✓
VPN Manager	✓
FortiGuard	
FortiManager HA	
FortiMeter	
FGT-VM License Activation	
Chassis Management	✓

## Language support

The following table lists FortiAnalyzer language support information.



Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓
French		✓
Hebrew		✓
Hungarian		✓
Japanese	✓	✓
Korean	✓	✓
Portuguese		✓
Russian		✓
Spanish		✓

To change the FortiAnalyzer language setting, go to *System Settings > Admin > Admin Settings*, in *Administrative Settings > Language* select the desired language from the drop-down list. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can create your own language translation files for these languages and import the language translation files into FortiAnalyzer by using one of the following commands:

```
execute sql-report import-lang <language name> <ftp> <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <sftp> <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <scp> <server IP address> <user name>
    <password> <file name>
execute sql-report import-lang <language name> <tftp> <server IP address> <file name>
```

For more information about commands, see the *FortiAnalyzer CLI Reference*.

## Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiManager, FortiWeb, FortiCache, and FortiSandbox models and firmware versions can log to a FortiAnalyzer appliance running version 6.0.0. Please ensure that the log devices are supported before completing the upgrade.



Software license activated LENC devices are supported, if their platforms are in the supported models list. For example, support of FG-3200D indicates support of FG-3200D-LENC.

**FortiGate models**

Model	Firmware Version
<b>FortiGate:</b> FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240-POE, FG-280D-POE, FG300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600D, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E <b>FortiGate 5000 Series:</b> FG-5001D, FG-5001E, FG-5001E1 <b>FortiGate DC:</b> FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC <b>FortiGate Hardware Low Encryption:</b> FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC <b>Note:</b> All license-based LENC is supported based on the FortiGate support list. <b>FortiWiFi:</b> FWF-30D, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-90D, FWF-90D-POE, FWF-92D <b>FortiGate VM:</b> FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZUREONDEMAND, FG-VM64-Azure, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM, FOS-VM64-Xen <b>FortiGate Rugged:</b> FGR-30D, FGR-35D, FGR-60D, FGR-90D	6.0

Model	Firmware Version
<b>FortiGate:</b> FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-POE, FG-60E-DSL, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240-POE, FG-280D-POE, FG-300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E, <b>FortiGate 5000 Series:</b> FG-5001C, FG-5001D, FG-5001E, FG-5001E1 <b>FortiGate DC:</b> FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815D-DC <b>FortiGate Hardware Low Encryption:</b> FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC <b>Note:</b> All license-based LENC is supported based on the FortiGate support list. <b>FortiWiFi:</b> FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D <b>FortiGate VM:</b> FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-Azure, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOSVM64, FOSVM64-KVM, FOS-VM64-Xen <b>FortiGate Rugged:</b> FGR-30D, FGR-35D, FGR-60D, FGR-90D	5.6

Model	Firmware Version
<b>FortiGate:</b> FG-30D, FG-30D-POE, FG-30E, FG-30E-3G4G-INTL, FG-30E-3G4G-NAM, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-200E, FG-201E, FGT-300D, FGT-300E, FGT-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E, FG-2000E, FG-2500E <b>FortiGate 5000 Series:</b> FG-5001C, FG-5001D, FG-5001E, FG-5001E1 <b>FortiGate 7000 Series:</b> FG-7030E-Q, FG-7030E-S, FG-7040E-1, FG-7040E-2, FG-7040E-3, FG-7040E-4, FG-7040E-5, FG-7040E-6, FG-7040E-8, FG-7040E-8-DC, FG-7060E-1, FG-7060E-2, FG-7060E-3, FG-7060E-4, FG-7060E-5, FG-7060E-6, FG-7060E-8 <b>FortiGate DC:</b> FG-80C-DC, FG-600C-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1500D-DC, FG-3000D-DC, FG-3100D-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3800D-DC, FG-3810D-DC, FG-3815DC <b>FortiGate Hardware Low Encryption:</b> FG-80C-LENC, FG-100D-LENC, FG-600C-LENC, FG-1000C-LENC <b>Note:</b> All license-based LENC is supported based on the FortiGate support list. <b>FortiWiFi:</b> FWF-30D, FWF-30D-POE, FWF-30E, FWF-30E-3G4G-INTL, FWF-30E-3G4G-NAM, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E-DSL, FWF-60E, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D <b>FortiGate VM:</b> FG-VM, FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-XEN, FG-VMX-Service-Manager, FOS-VM64, FOS-VM64-KVM <b>FortiGate Rugged:</b> FGR-30D, FGR-30D-ADSL-A, FGR-35D, FGR-60D, FGR-90D	5.4

Model	Firmware Version
<b>FortiGate:</b> FG-20C, FG-20C-ADSL-A, FG-30D, FG-30D-POE, FG-40C, FG-60C, FG-60C-POE, FG-60C-SFP, FG-60D, FG-60D-3G4G-VZW, FG-60D-POE, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-90D, FG-90D-POE, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-110C, FG-111C, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200B, FG-200B-POE, FG-200D, FG-200D-POE, FG-240D, FG-240D-POE, FG-280D-POE, FG-300C, FG-300D, FG-310B, FG-311B, FG-400D, FG-500D, FG-600C, FG-600D, FG-620B, FG-621B, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1240B, FG-1500D, FG-1500DT, FG-3000D, FG-3016B, FG-3040B, FG-3100D, FG-3140B, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3700DX, FG-3810A, FG-3810D, FG-3815D, FG-3950B, FG-3951B <b>FortiGate 5000 Series:</b> FG-5001A, FG-5001A-SW, FG-5001A-LENC, FG-5001A-DW-LENC, FG-5001A-SW-LENC, FG-5001B, FG-5001C, FG-5001D, FG-5101C <b>FortiGate DC:</b> FG-80C-DC, FG-300C-DC, FG-310B-DC, FG-600C-DC, FG-620B-DC, FG-621B-DC, FG-800C-DC, FG-800D-DC, FG-1000C-DC, FG-1240B-DC, FG-1500D-DC, FG-3000D-DC, FG-3040B-DC, FG-3100D-DC, FG-3140B-DC, FG-3200D-DC, FG-3240C-DC, FG-3600C-DC, FG-3700D-DC, FG-3810A-DC, FG-3810D-DC, FG-3815D-DC, FG-3950B-DC, FG-3951B-DC <b>FortiGate Low Encryption:</b> FG-20C-LENC, FG-40C-LENC, FG-60C-LENC, FG-80C-LENC, FG-100D-LENC, FG-200B-LENC, FG-300C-LENC, FG-310B-LENC, FG-600C-LENC, FG-620B-LENC, FG-1000C-LENC, FG-1240B-LENC, FG-3040B-LENC, FG-3140B-LENC, FG-3810A-LENC, FG-3950B-LENC <b>FortiWiFi:</b> FWF-20C, FWF-20C-ADSL-A, FWF-30D, FWF-30D-POE, FWF-40C, FWF-60C, FWF-60CM, FWF-60CX-ADSL-A, FWF-60D, FWF-60D-3G4G-VZW, FWF-60D-POE, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D <b>FortiGate Rugged:</b> FGR-60D, FGR-100C <b>FortiGate VM:</b> FG-VM, FG-VM64, FG-VM64-AWSONDEMAND, FG-VM-Azure, FG-VM64-HV, FG-VM64-KVM, FG-VM64-XEN <b>FortiSwitch:</b> FS-5203B, FCT-5902D	5.2

### FortiCarrier Models

Model	Firmware Version
<b>FortiCarrier:</b> FCR-3000D, FCR-3100D, FCR-3200D, FCR-3700D, FCR-3700DX, FCR-3800D, FCR-3810D, FCR-3815D, FCR-5001C, FCR-5001D, FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3240C, FCR-3600C, FCR-3700D-DC, FCR-3810D-DC, FCR-5001C <b>FortiCarrier DC:</b> FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3240C-DC, FCR-3600C-DC, FCR-3700D-DC, FCR-3810D-DC, FCR-3815D-DC <b>FortiCarrier VM:</b> FCR-VM, FCR-VM64, FCR-VM64-AWS, FCR-VM64-AWSONDEMAND, FCR-VM64-HV, FCR-VM64-KVM	5.4

Model	Firmware Version
<b>FortiCarrier:</b> FCR-3000D, FCR-3100D, FCR-3200D, FCR-3240C, FCR-3600C, FCR-3700D, FCR-3700DX, FCR-3810A, FCR-3810D, FCR-3815D, FCR-3950B, FCR-3951B, FCR-5001A, FCR-5001B, FCR-5001C, FCR-5001D, FCR-5101C, FCR5203B, FCR-5902D <b>FortiCarrier DC:</b> FCR-3000D-DC, FCR-3100D-DC, FCR-3200D-DC, FCR-3700D-DC, FCR-3810D-DC <b>FortiCarrier Low Encryption:</b> FCR-5001A-DW-LENC <b>FortiCarrier VM:</b> FCR-VM, FCR-VM64, FCR-VM64-HV, FCR-VM64-KVM, FCR-Vm64-XEN, FCR-VM64-AWSONDEMAND	5.2

### FortiDDoS models

Model	Firmware Version
<b>FortiDDoS:</b> FI-200B, FI-400B, FI-600B, FI-800B, FI-900B, FI-1000B, FI-1200B, FI-2000B	4.2, 4.1, 4.0

### FortiAnalyzer models

Model	Firmware Version
<b>FortiAnalyzer:</b> FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, and FAZ-3900E.  <b>FortiAnalyzer VM:</b> FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, and FAZ-VM64-XEN (Citrix XenServer and Open Source Xen).	5.6
<b>FortiAnalyzer:</b> FAZ-200D, FAZ-300D, FAZ-400E, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-2000E, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, and FAZ-4000B.  <b>FortiAnalyzer VM:</b> FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-XEN (Citrix XenServer and Open Source Xen), FAZ-VM64-KVM, and FAZ-VM64-AWS.	5.4
<b>FortiAnalyzer:</b> FAZ-100C, FAZ-200D, FAZ-200E, FAZ-300D, FAZ-400C, FAZ-400E, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-3900E, FAZ-4000B <b>FortiAnalyzer VM:</b> FAZ-VM, FAZ-VM-AWS, FAZ-VM64, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM64-KVM, FAZ-VM64-XEN	5.2
<b>FortiAnalyzer:</b> FAZ-100C, FAZ-200D, FAZ-200E, FAZ-300D, FAZ-400B, FAZ-400C, FAZ-400E, FAZ-1000B, FAZ-1000C, FAZ-1000D, FAZ-1000E, FAZ-2000A, FAZ-2000B, FAZ-3000D, FAZ-3000E, FAZ-3000F, FAZ-3500E, FAZ-3500F, FAZ-4000A, FAZ-4000B <b>FortiAnalyzer VM:</b> FAZ-VM, FAZ-VM64, FAZ-VM64-AWS, FAZ-VM64-Azure, FAZ-VM64-HV, FAZ-VM-KVM, FAZ-VM-XEN	5.0

**FortiMail models**

Model	Firmware Version
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-2000E, FE-3000C, FE-3000D, FE-3000E, FE-3200E, FE-5002B <b>FortiMail Low Encryption:</b> FE-3000C-LENC <b>FortiMail VM:</b> FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.3.7
<b>FortiMail:</b> FE-60D, FE-200D, FE-200E, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5002B <b>FortiMail VM:</b> FE-VM64, FE-VM64-HV, FE-VM64-XEN	5.2.8
<b>FortiMail:</b> FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-400E, FE-1000D, FE-2000B, FE-3000C, FE-3000D, FE-5001A, FE-5002B <b>FortiMail VM:</b> FE-VM64	5.1.6
<b>FortiMail:</b> FE-100C, FE-200D, FE-200E, FE-400B, FE-400C, FE-1000D, FE-2000A, FE-2000B, FE-3000C, FE-3000D, FE-4000A, FE-5001A, FE-5002B <b>FortiMail VM:</b> FE-VM64	5.0.10

**FortiSandbox models**

Model	Firmware Version
<b>FortiSandbox:</b> FSA-1000D, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D <b>FortiSandbox VM:</b> FSA-VM	2.4.0 2.3.2
<b>FortiSandbox:</b> FSA-1000D, FSA-3000D, FSA-3500D <b>FortiSandbox VM:</b> FSA-VM	2.2.0 2.1.0
<b>FortiSandbox:</b> FSA-1000D, FSA-3000D <b>FortiSandbox VM:</b> FSA-VM	2.0.0 1.4.2
<b>FortiSandbox:</b> FSA-1000D, FSA-3000D	1.4.0 and 1.4.1 1.3.0 1.2.0 and later

**FortiSwitch ACTA models**

Model	Firmware Version
<b>FortiController:</b> FTCL-5103B, FTCL-5902D, FTCL-5903C, FTCL-59	5.2.0
<b>FortiSwitch-ATCA:</b> FS-5003A, FS-5003B <b>FortiController:</b> FTCL-5103B, FTCL-5903C, FTCL-5913C	5.0.0
<b>FortiSwitch-ATCA:</b> FS-5003A, FS-5003B	4.3.0 4.2.0

**FortiWeb models**

Model	Firmware Version
<b>FortiWeb:</b> FWB-2000E	5.6.0
<b>FortiWeb:</b> FWB-100D, FWB-400C, FWB-400D, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-3010E, FWB-4000C, FWB-4000D, FWB-4000E	5.5.3
<b>FortiWeb VM:</b> FWB-VM-64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV, FWB-KVM, FWB-AZURE	
<b>FortiWeb:</b> FWB-100D, FWB-400C, FWB-1000C, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E	5.4.1
<b>FortiWeb VM:</b> FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, FWB-HYPERV	
<b>FortiWeb:</b> FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E	5.3.8
<b>FortiWeb VM:</b> FWB-VM64, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR, and FWB-HYPERV	
<b>FortiWeb:</b> FWB-100D, FWB-400B, FWB-400C, FWB-1000B, FWB-1000C, FWB-1000D, FWB-3000C, FWB-3000CFSX, FWB-3000D, FWB-3000DFSX, FWB-3000E, FWB-4000C, FWB-4000D, FWB-4000E	5.2.4
<b>FortiWeb VM:</b> FWB-VM64, FWB-HYPERV, FWB-XENAWS, FWB-XENOPEN, FWB-XENSERVR	

**FortiCache models**

Model	Firmware Version
<b>FortiCache:</b> FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3900E	4.1
<b>FortiCache VM:</b> FCH-VM64, FCH-KVM	
<b>FortiCache:</b> FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3900E	4.0
<b>FortiCache VM:</b> FCH-VM64	



# Resolved Issues

The following issues have been fixed in FortiAnalyzer version 6.0.0. For inquiries about a particular bug, please contact [Customer Service & Support](#).

## Device Manager

Bug ID	Description
469992	When there are multiple VDOMs for a device, only a single VDOM's log files are deleted when quota policy is enforced.
463465	Device Manager only shows one of the HA members when displaying the topology for CSF.
458857	After exported PDF in FortiView, the generated report does not show the correct color for the bar graph.
462507	FortiAnalyzer fails to register CSF when password contains special character.
469903	FortiGate cluster devices with same group name may be mixed up under Device Manager.

## FortiView

Bug ID	Description
365200	Scroll bar may be missing in the Resource Usage line chart.
454990	Policy name changes may not be updated in the list in <i>Traffic &gt; Policy Hits</i> page.

## Log View

Bug ID	Description
459304	Reports exported from FortiView does not have application icons or some fields are missing.
459487	The search combo box for column settings loses focus after being clicked or scrolling through the list.
459802	Custom View does not save the + sign defined within filter.

Bug ID	Description
406861	fazsvcd may crash when users import .gz raw log file.
472840	Right-click traffic log filter may not work for action accept.
473717	Log search may not work for <i>System &gt; Log disk events</i> from FortiGate.
470516	oftpd process may stop responding.
471259	Browse Time may not be calculated correctly.
473170	There may be an error when users try to save a custom view with special characters in catdesc.
471932	The search window may take up a large part of the screen.
472240	Under Log View, FortiAuthenticator events may not be filtered using the <i>Message</i> field.
465736	Syslog forwarded from Log Forward may contain duplicated date and time fields.
4144263	Hostname may contain user information in Endpoints.
451773	Log filter for User in Event – VPN may not work.
446799	The format of syslog sent by log-forward may be changed.
455956	In the SSL & Dial IPsec page, <i>Sorted by Connection Time</i> may not work.

## Reports

476645	SFTP password length is limited to 31 characters.
473771	Report Filters may not contain FortiMail log fields.
434087	FortiAnalyzer should not zip and encode for reports that are generated in CSV or XML format.
460221	The duration time of VPN users does not match that in FortiView.
392096	The bar representing Bandwidth may overlap with its text in the Top 5 Users by Bandwidth report.

## System Settings

378165	When Event logs are filtered by 'NOT' Sub Type, the results are still the same as Sub Type.
455634	FortiAnalyzer may generate excessive warning messages in alert console when log rate exceeds the peak rate.
469015	Incorrect local event log message may be generated when one of the FortiGate device in an HA cluster hasn't sent logs for some time.

## NOC

Bug ID	Description
454041	Bar chart should use Bandwidth as the y-axis instead of Sessions when data is sorted by Bandwidth.
457879	Widgets in dashboard in NOC may not backup.
465170	When switching theme from Day to Night, Top Application Tree map may not properly display icons and label.

## Others

Bug ID	Description
454193	FortiAnalyzer may keep generating <code>hcache</code> for multiple ADOMs causing high IO usage.

## System Settings

Bug ID	Description
463453	There is no local event log when a report output is to a remote FTP server.
467914	The value for received logs is incorrect in alert console when log exceeds the license limit.
467963	Alert console displays messages related to <code>sqllogd</code> daemon is suspended due to log aggregation.
417618	The IPsec VPN query results related to datasets may be incorrect.
440135	The VPN Traffic Usage Trend chart may not use increment bandwidth.

## Common Vulnerabilities and Exposures

Bug ID	Description
473376	FortiAnalyzer 6.0.0 is no longer vulnerable to the following CVE References: <ul style="list-style-type: none"><li>• CVE-2015-9251</li></ul> Visit <a href="https://fortiguard.com/psirt">https://fortiguard.com/psirt</a> for more information.

# Known Issues

The following issues have been identified in FortiAnalyzer version 6.0.0. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

## Device Manager

Bug ID	Description
482543	When adding a HA member to an existing device, Device Manager may show both devices with the same serial number.

## Event Management

Bug ID	Description
476489	Viewing the list of alerts triggered by traffic log with <code>catdesc</code> field will trigger system to return an error.
478209	Event filter may not work for some event handlers.
480476	Sorting by Severity may not work.
481556	Users may not be able to search for events.
481566	Event status may always be recognized as <i>Unhandled</i> instead of <i>Blank</i> .
483118	FortiAnalyzer may not be able to load data to display for Custom View.
483225	Right click menu may be missing from Custom View.
483572	Users may not be able to see avatars in the search when a user belongs to multiple end points.
483656	Users may not be able to see avatars on events triggered by FortiClient.
470373	During database rebuilds, alerts that are already triggered may be replayed again.

## FortiView

Bug ID	Description
476316	FortiAnalyzer should properly display IP address with port number under the Web Sites view.
473826	When FortiGate devices are in HA mode, there should not be duplicated IPv4 & IPv6 local policy 0 entries in Policies view.
473629	Web Sites view with the <i>Domain</i> filter applied should not show the entire threat list.
474061	When using wildcard expression for <code>srcip</code> with multiple subnets, search returns sporadic results.
484312	Top Threats may display threats as numerical values without any detailed information.
484761	Compromised Hosts may show many duplicate entries.
484821	Compromised Hosts may show blank entries for end users.

## Log View

Bug ID	Description
473907	FortiAnalyzer should not truncate syslog messages sent from Windows AD server using syslog agent.
479688	FortiAnalyzer may always show acknowledged events with duplicated End User entries. Also, UUID may be displayed as the Host Name.
480205	Dot and wildcard are automatically removed when searching text in advanced mode.
481771	FortiWeb logs cannot being received if encryption is enabled.
482909	Application Control Logs and FortiView shows different information when inspecting GTP traffics.
483420	FortiAnalyzer may return an error when a user exports a report from IOC drilldown table.
483611	Column can be misaligned where there are some entries containing attachments.
473907	FortiAnalyzer should not truncate syslog messages sent from the Windows AD server using the syslog agent.

## NOC

Bug ID	Description
483683	The Security Rating Score may not be correct when there is a FortiGate HA failover.
484196	The CVE links under the Critical Vulnerabilities panel may not work in <i>SOC View &gt; Vulnerabilities Monitor</i> page.
484693	The <i>Compromised Hosts Incidents</i> widget displays the <i>No Data</i> warning even when there is data showing in the widget.

## Reports

Bug ID	Description
434272	PDF reports size may be bigger after upgrade.
470616	Rendering of tables in PDF report may display overlapping entries.
476000	Reports may not show the full results within specified time period.
480088	Export template under the CLI may not work.
483778	The Bandwidth Summary graph may not be accurate if there are more than twenty eight days included within a report.
469541	Users cannot import reports from version 5.0 to 6.0.
470616	Entries may overlap in the reports generated in PDF format.
484350	The <i>Proxy Applications</i> and <i>Remote Access Application</i> charts in the Cyber Threat Assessment report turns may not show any data after upgrading from 5.6.0.
484863	All report names with underline should concatenated with <code>uuid</code> .

## System settings

Bug ID	Description
476109	FortiAnalyzer may forward logs with incorrect <code>logid</code> .
476701	Log forwarding sends <code>poluuid</code> value without closing double quotes.
479159	Devices may not display in logging topology when device traffic option is selected.

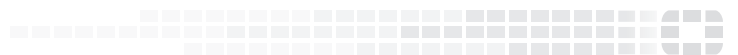
Bug ID	Description
484194	Forwarded logs should not include excluded log fields.
470489	Under <i>Storage Info</i> , columns may not be displayed properly when doing a search.
474066	When an administrator profile is configured with Read-Write permission for Reports and Read-Only for System Settings, administrators associated with the profile cannot preview or save a chart using the chart builder.
484349	Fetch session may be paused after approval.

## Others

Bug ID	Description
482508	Console may continuously show the error message: <i>Audit rpt format error</i> .
482751	HA primary unit's HA daemon uses 100% resource on a single CPU core.
483897	Users may not be able to search HA traffics by device name via JSON APIs.
469050	The XML API, <code>getFazGeneratedReport</code> , cannot return report name that contains Unicode.
483917	FortiAnalyzer may stuck when rebuilding the database. <b>Workaround:</b> Run the <code>diagnose test application sqllogd 99</code> CLI command.



**FORTINET®**



Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.